US-CHINA

# TikTok bills could dangerously expand national security state

Congressional proposals to address Chinese ownership of the popular app go well beyond the hearing soundbites. Let's explore.

MARCH 29, 2023

Written by Marcus Stanley

TikTok has been all the rage in Washington lately. Not for the reasons which lead some 150 million Americans to use it, but because of the rush by politicians to try to ban the app, which is owned by ByteDance, a Chinese company.

Two major bills that would impose sweeping restrictions on Chinese-owned software are working their way through the House (HR 1153) and Senate (S 686), while TikTok CEO Shou Zi Chew was recently brought before the House Commerce Committee for hostile questioning. The executive branch is also seeking to force ByteDance to sell the app to an American owner, against Chinese opposition.

Those raising the alarm about Chinese ownership of TikTok cite invasive surveillance practices, privacy violations created by excessive collection and exploitation of user data, addictive design features, and harmful content. But all of these disturbing characteristics are also ubiquitous features of American-owned big tech apps ranging from Google to Facebook to Instagram, and were in many ways pioneered by American Silicon Valley companies.

In the case of TikTok, the claim is that Chinese ownership makes these problems particularly harmful because Chinese intelligence services can access user data and technologies owned by Chinese companies such as ByteDance. Some also go further by claiming that TikTok could be used to compromise the security of devices on which it is installed.

It remains somewhat unclear exactly how the Chinese government would use TikTok to harm American users in ways that other big tech apps do not. This raises the question of whether what is needed is not an attack on TikTok but a broader effort to protect user privacy and protect children from harmful content on big tech apps in general.

But an examination of the two "TikTok bills" working their way through Congress raises another question. Is TikTok being used as the wedge for a much broader effort to restrict companies owned by rival nations across the entire information technology sector? And does this effort threaten American civil liberties and risk government overreach?

HR 1153, the DATA Act, which recently passed the House Foreign Affairs Committee, is almost surreal in some of its implications. Section 102 of the bill, oriented toward penalties on U.S. citizens, would require the secretary of the treasury to ban any U.S. financial transactions by any American who had knowingly transferred sensitive personal information to any entity owned by or even "subject to the influence of" China.

Since the definition of "sensitive personal information" is very broad, this could mean that any company or individual who had, for example, forwarded emails or shared health insurance information with a company that had even partial Chinese ownership could find themselves banned from financial transactions. Their assets would be effectively frozen — for example, they would be unable to use their credit cards or access cash in their bank accounts.

Title II of the bill focuses on foreign jurisdictions. It would require the U.S. government to freeze all U.S. assets of a foreign person anywhere in the world who "operates, directs, or otherwise deals in" a connected software application that is Chinese owned or "subject to the influence of" China, if such software facilitates Chinese military, surveillance, or censorship activities, or involves Chinese access to recommendation algorithms that could manipulate content.

This incredibly broad prohibition, connected to extreme penalties, would in effect make it a priority of the U.S. government to try to ban the use of much Chinese software anywhere in the world, including in nations that are allies or potential allies.

Many of the problems with HR 1153 were pointed out by Rep. Gregory Meeks (D-N.Y.) and other Democratic members of the House Foreign Affairs Committee during the committee debate on the bill, and the bill passed on a partisan vote. This makes it less likely that it will become law.

But that's not true of S 686, the RESTRICT Act, the Senate "TikTok bill," which has significant momentum toward passage. S 686 has 21 bipartisan co-sponsors and has been endorsed by the Biden administration. The bill would grant the executive branch unprecedented new national security powers over commerce in information and communication technologies, and by extension, speech.

The Restrict Act requires the executive branch to prohibit or otherwise "mitigate" any transaction or activity in information and communications technologies by companies controlled by a "foreign adversary," if the secretary determines that such a transaction poses any risk to U.S. national security.

The bill grants the president a wide range of civil and criminal options to enforce such mitigation, including forced divestment of assets, seizure of assets, and subpoenas for information. Under Section 12 of the bill, legal avenues to contest such actions are limited to rapid and direct constitutional challenges in the U.S. Court of Appeals for the District of Columbia.

The initial list of "foreign adversaries" in the bill includes China, Cuba, Russia, Iran, Venezuela, and North Korea.The executive branch could add additional foreign adversary nations at will. This choice could only be overridden by a majority vote of both houses of Congress.

While these powers would be discretionary, and could theoretically be used in a restrained and measured way, there is no guarantee they would be. In effect, this bill would ban ownership of any widely used information and communications technologies within the U.S. market by foreign nations viewed as adversaries of the U.S. At the very least, such technologies could be subject to censorship at will.

This could have significant ramifications internationally and domestically. We may see retaliatory bans on the use of U.S. software and communications technologies in foreign countries targeted as "adversary nations" — possibly the beginning of the division of the world into rival information technology spheres protected by "great firewalls" like that imposed by China.

Domestically, Section 11 of the bill establishes draconian penalties for American citizens who violate it by attempting to evade or help others to evade new restrictions on foreign-owned information and communications technologies. While it is somewhat ambiguous how far this could go, it could lead to American citizens being prosecuted for accessing information on foreign-owned technology platforms such as WeChat.

This kind of censorship, based on foreign ownership rather than content, has not been tested under First Amendment law, but it could have profound implications. The ACLU has already stated its opposition to the bill on freedom of expression grounds.

In the end, it seems that there should be much easier ways to prevent Chinese government access to private user data on TikTok. But for those who wish to expand the power of the national security state, the sweeping nature of these proposals might be a feature, not a bug.